

WHAT IS CLAIMED IS:

1. A license compliance verification system, comprising:

a license manager that internally monitors use of licensed property, intended to be used by licensed users, and gathers data on the usage of the licensed property including by reference to a plurality of licensors of the license property; and

monitoring software that interfaces with the license manager and extracts from it licensor-specific data and authenticates the retrieved data such that licensors are assured, based on a set of rules, that data gathered by the license manager has not been altered or improperly deleted prior to its being provided to licensors.

2. The license compliance verification system of claim 1, in which the licensed property comprises computer software.

3. The license compliance verification system of claim 1, in which the monitoring software includes a facility that enables users to review data before it is sent to licensors and prevents users from modifying such data.

4. The license compliance verification system of claim 1, in which the license manager includes a facility that accepts passwords and license certificates for authorizing usage of respective ones of the licensed property.

5. The license compliance verification system of claim 1, in which the gathered data comprises out-of-compliance data.

6. The license compliance verification system of claim 1, in which the gathered data comprises license certificate modification data.

7. The license compliance verification system of claim 1, in which the monitoring software includes a facility that enables licensors to directly and remotely provide instructions to the monitoring software.

8. The license compliance verification system of claim 1, in which direct access to the monitoring software is granted to an agent operating on behalf of a licensor but which is active on a user's computer.

9. The license compliance verification system of claim 1, further including an operator control facility that enables controlling the monitoring software to carry out a data gathering task based on selection criteria and the selection criteria includes at least identification of products or licensors.

10. The license compliance verification system of claim 1, in which the monitoring software is operable on a time scheduling basis.

11. The license compliance verification system of claim 1, further including a facility for creating a new symmetric encryption key for encrypting the data to be transferred to licensors.

12. The license compliance verification system of claim 11, including a facility that encrypts the symmetric encryption key using a public key of a licensor.

13. The license compliance verification system of claim 11, including a facility that encrypts the symmetric encryption key using a public key of a user.

14. The license compliance verification system of claim 1, further including an authenticating facility which is operable as a part of the monitoring software and which authenticates data that is gathered for a licensor, to prevent tampering with such data.

15. The license compliance verification system of claim 14, in which the authentication comprises a message digest and the message digest is a data digest selected from the group consisting of a hash value or an arithmetic total computed from encrypted data which is then encrypted using a private key specific to the monitoring software.

16. The license compliance verification system of claim 1, in which the licensed property is selected from a property group consisting of: licensed software, trade secrets, copyrighted music, copyrighted books, copyrighted photos, copyrighted movies, and copyrighted videos.

17. A method for verifying compliance with license conditions, the method comprising the steps of:

operating a license manager so as to internally monitor use of licensed property, intended to be used by licensed users, and gathering data on the usage of the

licensed property including by reference to respective licensors of the licensed property; and

10 extracting, from data logged by the license manager, licensor-specific data; and authenticating at least portions of the retrieved data in preparation for forwarding the retrieved data to one or more licensors, so as to assure that data gathered by the license manager has not been altered or improperly deleted prior to its being provided to licensors.

18. The method of claim 17, in which licensed property comprises computer software.

19. The method of claim 17, further including enabling users to review data before it is sent to licensors and preventing users from improperly modifying such data.

20. The method of claim 17, including operating the license manager to accept passwords and license certificates for authorizing usage of respective ones of the licensed property.

21. The method of claim 17, including retrieving from

the license manager out-of-compliance data.

22. The method of claim 17, in which the gathered data comprises license certificate modification data.

23. The method of claim 17, including enabling licensors to directly and remotely provide instructions which affect the retrieving of data from the license manager.

24. The method of claim 23, further including operating an agent on behalf of the licensor which is active on a user's computer.

25. The method of claim 17, further including controlling the retrieving of data from the license manager based on selection criteria that select information at least on a basis of identifying licensors or licensed products.

26. The method of claim 17, further including retrieving data from the license manager by reference to time periods over which such data has been initially collected.

27. The method of claim 17, further including creating a new symmetric encryption key for encrypting the data to be transferred to licensors.

28. The method of claim 27, including encrypting the symmetric encryption key using the public key of the licensor.

29. The method of claim 27, including encrypting the symmetric encryption key using the public key of a user.

30. The method of claim 17, further including authenticating retrieved data.

31. The method of claim 30, including employing an authentication process which comprises including a message digest, said message digest being a data digest selected from a group consisting of a hash value or an arithmetic total computed from the encrypted data which is encrypted using a private key.

32. The method of claim 17, in which the licensed property is selected from a property group consisting of: licensed software, trade secrets, copyrighted music,

copyrighted books, copyrighted photos, copyrighted movies
5 and copyrighted videos.

33. The method of claim 28, further including
encrypting the symmetric encryption key which has been
encrypted using the public key of the licensor, with a
user's public key and subsequently providing such twice
5 encrypted information to a respective user.

34. The license compliance verification system of
claim 12, including a facility that encrypts the symmetric
encryption key, which has been encrypted using the public
key of the licensor, with a user's public key and
subsequently providing such twice encrypted information to
a respective user.

35. The license compliance verification system of
claim 1, further including a central clearinghouse
facility, the monitoring software accumulating licensor-
specific data pertaining to a plurality of licensors and
transmitting the same to the central clearinghouse
5 facility, the clearinghouse facility consolidating, sorting
and providing the licensor-specific data according to
licensors.

36. The license compliance verification system of claim 35, in which the monitoring software and the central clearinghouse facility interact with each other automatically.

37. The license compliance verification system of claim 35, in which the monitoring software and the central clearinghouse facility interact with each other in response to prompting by specific licensors.

38. The method of claim 17, further including accumulating the licensor-specific data relative to a plurality of licensors and transmitting the same to a central clearinghouse facility, the central clearinghouse facility consolidating, sorting and providing the licensor-specific data according to licensors.

39. The method of claim 38, including transmitting the licensor-specific data to the central clearinghouse facility automatically.

40. The method of claim 38, including transmitting the licensor-specific data to the central clearinghouse facility in response to prompting by specific licensors.